AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with darin.dowd@iCloud.com that is currently within law enforcement custody at the ATF Milwaukee Field Office.

Case No. 22-M-300 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 1-17-22 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries, U.S. Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 1-3-22 11:30 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with darin.dowd@iCloud.com that is currently within law enforcement custody at the ATF Milwaukee Field Office.

ATTACHMENT B
Particular Things to be Seized

1. Information to be disclosed by Apple (Provider)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved (reference number 6262734) pursuant to a request made under 18 U.S.C. § 2703(f) on July 21, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from 01/01/2021 to the present:

- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to

access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

- The contents of all emails associated with the account from 01/01/21 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- The contents of all instant messages associated with the account 01/01/21 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant

message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

- All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- All records pertaining to the types of service used;
- All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal import of ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); and 18 U.S.C § 545 (Smuggling), those violations involving Darin DOWD and occurring after 01/01/21, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records containing the sale/purchase order of ammunition in a illegal format that is intended for the military/law enforcement that would not be for public use. Records can be contained in emails, text messages, SMS messages, iMessages, etc.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to the conspiracy and illegal importation of ammunition, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with darin.dowd@iCloud.com that is currently within law enforcement custody at the ATF Milwaukee Field Office.

Case No. 22-M-300 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 371; 18 U.S.C. § 922(l); 18 U.S.C § 542; 18 U.S.C § 545	Conspiracy; illegal import of ammunition; entry of goods by means of false statements; smuggling.

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ALEXANDER ERLIEN Digitally signed by ALEXANDER ERLIEN Date: 2022.01.03 10:47:52 -06'00'

Applicant's signature

Special Agent Alexander Erlien, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 1-3-22

Stephen C. Dries

Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Alexander Erlien, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a supplemental examination and extraction of electronically stored information described in Attachment B, previously extracted from an iCloud account. The information needing extraction is already in law enforcement custody.

2. On November 19, 2021, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) obtained a federal search warrant for the contents of the Apple iCloud account darin.dowd@iCloud.com. The warrant was authorized by the Honorable Judge Stephen Dries. The account is associated with Darin DOWD (W/M, DOB: 05/19/1991). In an abundance of caution, the Government seeks another warrant to seize and search the same forensic extraction of the iCloud account for electronically stored information related to an investigation into the impersonation of an officer or employee of the United States (18 U.S. Code § 912) by Jacob DOWD, Darin DOWD, and other known and unknown individuals.

3. I have been a Special Agent with the ATF since September 26, 2018. I was previously employed as Police Officer for the City of Janesville, Wisconsin for approximately five and a half years, and prior to that, I was an Officer in the United States Navy for approximately five years. I have a bachelor's degree in philosophy from the University of Wisconsin – Madison. I have been involved in numerous investigations involving violations of firearms laws, drug trafficking, human trafficking,

and drug possession, resulting in the arrest of numerous criminal defendants and the seizure of illegal firearms and illicit controlled substances.

4. I have received training in the investigation of unlawful possession of firearms and possession of firearms by prohibited persons, as well as drug trafficking and related offenses. I have been trained regarding these offenses and has arrested individuals for federal firearms related offenses, as well as drug trafficking offenses. I have also investigated drug trafficking offenses at the state and federal level, including violations of Title 21, United States Code, Sections 841, 846, and 856. I know from training and experience that those that commit crimes commonly communicate, photograph, videotape, and organize using electronic devices, including by phone call, text message, electronic mail, messaging application, and social media.

5. I have participated in numerous investigations involving the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. I have also participated in investigations involving the use of historical and prospective location information to identify targets, map patterns of travel, corroborate other evidence, and apprehend persons to be arrested. On numerous occasions, this electronic evidence has provided proof of the crimes being investigated and corroborated information already known or suspected by law enforcement. During the course of my investigations, I have regularly used electronic evidence relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

6. I have participated in the execution of numerous search warrants in which weapons, narcotics, and/or evidence of drug trafficking were seized. I am familiar with

the different types and calibers of firearms and ammunition commonly possessed for illegal purposes, as well as the methods used to conduct narcotics trafficking.

7. I have had both formal training and have participated in numerous complex drug trafficking investigations. I have received training in the investigation of unlawful possession of firearms, drug trafficking, money laundering, financial investigations, and computer crimes. My training and experience include the following:

a. Through informant interviews and extensive debriefings of individuals involved in firearms and drug trafficking, I have learned about the manner in which individuals and organizations finance, source, purchase, transport, and distribute firearms and controlled substances in Wisconsin, throughout the United States, and internationally.

b. I have used my training and experience to locate, identify, and seize multiple types of firearms, narcotics, drugs, drug proceeds, and drug contraband.

c. I have also relied upon informants to obtain firearms and controlled substances from firearms and drug traffickers and have made undercover purchases of firearms and controlled substances.

d. I have extensive experience conducting street surveillance of individuals engaged in firearm and drug trafficking. I have participated in the execution of numerous search warrants where firearms, controlled substances, drug paraphernalia, and drug trafficking records were seized.

e. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, cocaine, cocaine base (unless otherwise noted, all references to crack cocaine in this affidavit is cocaine base in the form of crack cocaine), ecstasy, and methamphetamine. I am familiar with the methods used by drug traffickers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances.

f. I am familiar with the language used over the telephone and other electronic communications to discuss firearm and drug trafficking and know that the language is often limited, guarded, and coded. I know the various code names used to describe firearms and

controlled substances. I also know that firearm and drug traffickers often use electronic devices (such as computers and cellular phones), electronic communication services (such as e-mail and messaging services), and social media to facilitate these crimes.

g. I know firearm and drug traffickers often register phones, mailboxes, bank accounts, electronic communication services, and other instrumentalities of drug trafficking in the names of others, also known as nominees, to distance themselves from instrumentalities used to facilitate drug trafficking.

h. I know that firearm and drug traffickers often use electronic equipment and wireless and landline telephones to conduct trafficking operations.

i. I know that firearm and drug traffickers often keep documents and records about the transportation, sourcing, ordering, sale, and distribution of controlled substances and firearms. I know these records can be kept on electronic devices or physical document. These items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control.

j. I know that firearm and drug traffickers often use their proceeds to purchase assets such as vehicles, property, and jewelry. I also know that firearm and drug traffickers often use nominees to purchase or title these assets in order to avoid scrutiny from law enforcement officials. I know that firearm and drug traffickers often secure proceeds from their illegal sales at locations within their dominion and control, such as their residences, businesses, other locations over which they maintain dominion and control and storage facilities, and in safes or other secure containers.

k. I know that firearm and drug traffickers often attempt to protect and conceal illegally obtained proceeds through money laundering, including but not limited to domestic and international banks, securities brokers, service professionals such as attorneys and accountants, casinos, real estate, shell corporations, business fronts, and otherwise legitimate businesses which generate large quantities of currency. I know it is common for firearm and drug traffickers to obtain, secrete, transfer, conceal, or spend proceeds, such as currency, financial instruments, precious metals, gemstones, jewelry, books, real estate, and vehicles. I know it is common for firearm and drug traffickers to maintain documents and records of these illegally obtained proceeds, such as bank records, passbooks, money drafts, transaction records, letters of credit, money orders, bank drafts, titles, ownership documents,

cashier's checks, bank checks, safe deposit box keys, money wrappers, and other documents relating to the purchase of financial instruments or the transfer of funds. I know firearm and drug traffickers often purchase or title assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are titled or purchases by nominees, the firearm and drug traffickers actually own, use, and exercise dominion and control over these assets. The aforementioned books, records, receipts, notes, ledgers, and other documents are often maintained where the traffickers have ready access. These may be stored in hard copy or soft copy on paper, computers, cellular devices, and other electronic media or electronic storage devices. These items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control.

l. I know firearm and drug traffickers maintain large amounts of currency, including in readily accessible financial accounts, to finance their ongoing drug business. I know that those involved in firearm and drug trafficking or money laundering keep records of their transactions. Because firearm and drug trafficking generates large sums of cash, traffickers often keep detailed records about the distribution of narcotics and the laundering of proceeds. I also know that firearm and drug trafficking and money laundering activities require the cooperation, association, and communication between and among a number of people. As a result, people who traffic in firearms, narcotics or launder money for such organizations possess documents that identify other members of their organization, such as telephone books, address books, handwritten notations, telephone bills, and documents containing lists of names and addresses of criminal associates. Such records also provide information about the identities of coconspirators who launder money and traffic drugs and firearms. I also know that firearm and drug traffickers commonly maintain addresses or telephone numbers which reflect names, addresses, or telephone numbers of their firearm and drug trafficking and money laundering associates in hard copy and soft copy on papers, books, computers, cellular devices, and other electronic media or electronic storage devices. Again, these items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control.

m. I know firearm and drug traffickers often use electronic devices, such as telephones, cellular devices, computers, and currency counting machines to generate, transfer, count, record, or store the

information described above and conduct firearm and drug trafficking and money laundering. I am familiar with computers, cellular devices, pagers, and other electronic media or electronic storage devices and their uses by firearm and drug traffickers to communicate with suppliers, customers, co-conspirators, and fellow traffickers. These devices often contain evidence of illegal activities in the form of communication records, voicemail, email, text messages, video and audio clips, location information, business records, and transaction records. I know firearm and drug traffickers take, store, preserve, or maintain photographs or videos of themselves, their associates, their property, their firearms, their drugs, and their drug proceeds. These traffickers usually maintain these photographs or videos on computers, cellular devices, and other electronic media or electronic storage devices. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime; and (2) the objects may have been used to collect and store information about crimes. I know the following information can be retrieved to show evidence of use of a computer or smartphone to further the drug trade: system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; computer media and any data contained within such media; operating system software, application or access program disks, manuals, books, brochures, or notes, computer access codes, user names, log files, configuration files, passwords, screen names, email addresses, IP addresses, and SIM cards.

n. I have participated in numerous firearm and drug trafficking investigations involving the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. This has led to evidence of the crimes under investigation and corroborated information already known or suspected by law enforcement. I have regularly used electronic evidence to find proof relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of suspects and conspirators.

o. I have also participated in the execution of numerous premises search warrants and arrests, where controlled substances, firearms, drug paraphernalia, drug proceeds, electronic devices, and records relating drug trafficking and drug proceeds were seized. I know that drug traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion

and control, firearms, ammunition, and records or receipts pertaining to such.

8. The facts in this affidavit come from my personal observations, my training and experience, and from information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S. Code § 912 (impersonating an officer or employee of the United States) have been committed and that evidence of those violations is contained in following Apple iCloud account:

- darin.dowd@icloud.com (Darin DOWD)

which is linked to the owner of United Forces Enterprises, Darin Dowd. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

1. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

2. On June 30, 2021, ATF Imports Branch flagged a suspicious ATF Form 6, Application for Permit and Importation of Firearms, Ammunition and Defense Articles submitted by Jacob Allen DOWD and Darin Wayne Dowd using an address of 2581 Nut

Tree Road, Suite A, Vacaville, CA, 95687 and an email address of "unitedforceenterprises@gmail.com". An open-source search revealed this as the physical and email address of Federal Firearms Licensee (FFL) United Forces Enterprises. The request was for the importation of 489,000 rounds of 7.62x 54mm armor piercing incendiary (API) rounds from Smart Energeo Sistemi in Pale, Bosnia and Herzegovina. Nonsporting ammunition may not be imported unless certain exceptions apply, including as relevant here for law enforcement use.

3. Your Affiant reviewed the application and observed the listed reason for importation was "LAW ENFORCEMENT SALES." Consistent with that stated reason for importation, the application was submitted along with a law enforcement exemption letter from the Town of Linn, Wisconsin, Police Department (TLPD). The exemption letter took the form of a purchase order on TLPD letterhead and signed by TLPD Chief James Bushey for 1.5 million rounds of 7.62x 54mm API ammunition. This furthered suspicions as TLPD is a very small department consisting of only six (6) full-time officers and five (5) reserve officers.

4. The application was digitally signed by "JACOB A DOWD" on 06/21/2021. The Form 6 listed "UNITEDFORCESENTERPRISES@GMAIL.COM" and "(707) 227-7590" as ways to contact DOWD.

5. Affiant reviewed the public website for United Forces Enterprises under URL https://unitedforces.com/. The website does not offer routine information as seen on traditional FFL and business websites such as contact information, company overview, or staff. The website appears to consist of only a welcome page. On the page, it states the company is, "providing comprehensive solutions all over the world."

Then it lists the following locations (as places they conduct business):

- United States: 50
- South America: 14
- Europe: 44
- Africa: 54

6. Following the above statement, the website lists the following ten (10) types of ammunition. Each ammunition has an expandable section marked by a "+" sign and provides generic information about the selected round. For example, the expanded information under the 9x19 Luger simply advises the round is used for short range distances and recommend for matches or practice. There is not information on how to obtain this product.

7. The website listed the following entities as partnered brands:

- ZVS Armory (an ammunition company located in Prievidza, Slovakia)
- STV Group (which is the largest producer of ammunition in the Czech Republic https://www.stvgroup.cz/en)
- Phoenix MN Ammunition (a private Romanian company that manufactures small caliber ammunition (https://www.phoenixms.ro/about-us/)
- Sumbro (a Macedonian ammunition manufacturer)
- ZSR (an ammunition and explosives company in Turkey https://zsrpatlayici.com/EN)

8. Although no contact information was found on the United Forces Enterprises website, an Instagram page for United Forces Enterprises was located at

https://www.instagram.com/unitedforcesenterprises/. As with all Instagram pages, there is an option to send a direct message to the user. The page provides a link to the webpage www.unitedforces.com. This is a dead link as the actual webpage address is https://unitedforces.com as mentioned in the above paragraph. Further, the Instagram page provided photographs that appear to be taken from the Internet. There are not photographs of employees, advertisements, or a business location provided. In your Affiant's training and experience this is unusual for an FFL's social media page.

9. Your Affiant also reviewed the public website for Alpha Omega Brokerage (https://aobrokerage.com/). The site claimed Alpha Omega Brokerage is the exclusive broker for United Forces Enterprises. The site advertised Chris Kyle American Sniper Brand Ammunition that is distributed by United Forces Enterprises and provided a catalog for ordering the ammunition. The final three pages of the catalog were an order form, a copy of the Federal Firearms License (FFL) for United Forces Enterprises, and a copy of the State of California Ammunition Vendor License for United Forces Enterprises. The website listed the following subjects as employees:

- Eli Lazar – President
- Joshua Beske - Director of Logistics/Military Liaison

10. Continuing on July 16, 2021, ATF agents traveled to Town of Linn Police Department to interview Chief James BUSHEY. In summary, Chief BUSHEY stated in August 2020 he was first visited in person by Jason WIEDENHOEFT (DOB: 07/1977) who identified himself as the salesman for United Forces Enterprises. WIEDENHOEFT worked for a different company that was contracted by United Forces Enterprises to secure these transactions (believed to Alpha Omega Brokerage). WIEDENHOEFT was

a local individual whom the Chief had known for a long time. WIEDENHOEFT and BUSHEY had also been roommates. Additionally, WIEDENHOEFT owns the Reaper Company, a nonprofit organization created to help veterans with PTSD, and Chief BUSHEY is on its board of directors.

11. Chief BUSHEY stated that WIEDENHOEFT advised Chief BUSHEY that United Forces Enterprises was a level ten (10) or level eleven (11) firearms dealer which allowed them to import firearms and ammunition from overseas. WIEDENHOEFT told Chief BUSHEY United Forces Enterprises were fulfilling large ammunition orders for Cabela's and other retailers which required the use of shipping containers. Chief BUSHEY reiterated that he had been told by several people this was "the gray area" the government worked under to acquire munitions.

12. WIEDENHOEFT explained his friend, known as "Josh" (suspected to be Joshua BESKE DOB: 02/1980) worked as private security for the United Forces Enterprises leadership - *i.e.*, Darin DOWD and Jacob DOWD and travels with them on security details. Chief BUSHEY advised that BESKE was a Marine Scout Sniper. Chief BUSHEY advised that he met BESKE through WIEDENHOEFT and believed him to live in northern Wisconsin.

13. Chief BUSHEY also explained there was some unknown middleman completing these deals for United Forces Enterprises who introduced WIEDENHOEFT to the DOWDs. Agents believe this to be Eli LAZAR.

14. Chief BUSHEY reiterated that he was told by several people this was "the gray area" the government worked under to acquire munitions. He indicated all these multiple levels of assurances made him feel comfortable about the transaction. Chief

Bushey figured if United Forces Enterprises was willing to give TLPD a $20,000 donation then the company must have been legitimate.

15. Affiant reviewed the purchase order signed and authorized by Chief James BUSHEY and dated June 16, 2021. The purchase order stated the following in summary:

- To: United Forces Enterprises, 2581 Nut Tree Road, Vacaville, Suite A, CA, 95687
- Order Date: 06/15/2021
- PO #: 00001
- Ship Date: 08/15/2021
- Order No. 1
- 7.62x54R API (armored piercing incendiary)
- Quantity: 1,500,000
- Cost: $0

16. Your Affiant knows that a police department exemption letter (in this case the purchase order signed by the chief on department letterhead) is considered valid by ATF for two years. Therefore, the quantity on the purchase order can be filled in multiple purchases at different times. The exemption letter only expires for the importer after two years or the quantity listed is met.

17. Affiant reviewed the ATF Form 6s that corresponded to the Chief BUSHEY's purchase order for the 7.62x54R API rounds. The following information was provided in summary:

ATF Form 6 (Permit No. 202106103)

- Applicant Name: Jacob and Darin DOWD
- Address: 2581 Nut Tree Road, Suite A, Vacaville, CA, 95687
- Foreign Seller: Smart Energo Sistemi of Bosnia and Herzegovina
- Ammunition Submitted: 489,000 rounds of Steel Core, Armor Piercing Incendiary (API), 7.62x54R
- Purpose of Importation: Law Enforcement
- Digitally Signed: Jacob DOWD, President on 06/29/2021
- Telephone: 707/227-7590
- Email: UNITEDFORCESENTERPRISES@GMAIL.COM

18. Chief BUSHEY stated that WIEDENHOEFT prepared the purchase order on TLPD letterhead that he mocked up. WIEDENHOEFT the purchase order to Chief BUSHEY to sign. Chief BUSHEY stated that he believed WIEDNHOEFT then passed the purchase order on to the DOWDs.

19. Chief BUSHEY also provided a second Linn Township Police Department Purchase Order that he did not sign that was requested by WIEDENHOEFT. The order listed a request for 3,000,000 rounds of 12.7X99 API Brass Case ammunition. This ammunition is commonly referred to in the United States as .50 caliber BMG and the API is an acronym for Armored Piercing Incendiary. This type of ammunition is used in firearms such as the Barrett M82 rifle and M2HB/M2 Browning belt-fed rifle. This is a large caliber weapon and is rarely, if ever, used for law enforcement purposes and even more rare to be an API round. The API 12.7x99 API round would be more commonly used in a firearm such as the M2HB/M2 belt-fed rifle. *The below photos are for reference for the types of firearms that can use API 12.7x99 API.*

Barrett .50 Caliber Rifle

Browning M2HB Belt-Fed .50 Caliber Rifle (stock photograph)

Barrett .50 Caliber rifle with .50 BMG Ammo (12.7x99) ammo

The purchase order listed the following information in summary:

- Order Date: 11/19/2020
- To: United Forces Enterprises, 2581 Nut Tree Road, Suite A, Vacaville, CA, 95687
- Description: 12.7x99 API Brass Case Ammunition
- Cost: $0.00

20. Chief BUSHEY advised he was first contacted by ATF agents outside of the Eastern District of Wisconsin prior to this interview regarding the TLPD purchase order that accompanied the United Forces Enterprises ATF Form 6 import application.

21. Following their conversation, he and WIEDENHOEFT exchanged text

messages regarding the ATF interaction beginning on June 30, 2021. WIEDENHOEFT advised Chief BUSHEY that ATF was going to call to ensure he approved the purchase order. On July 1, 2021, Chief BUSHEY told WIEDENHOEFT via text that ATF did call. WIEDENHOEFT asked Chief BUSHEY if the call was "an easy call or extensive" and explained he was "just curious so he could tell others what to expect." Chief BUSHEY advised WIEDENHOEFT that ATF advised the transaction "looked a bit odd that a small dept in WI was buying 1.5 million rounds of belt fed ammo." Chief BUSHEY explained he told ATF "… well if you have a fleet or (*sic*) f16's, then you'd know that is the minimum necessary to keep us going". WIEDENHOEFT replied, "Lol we shall see the cali boys said that they have had no issues with ATF on this". Affiant believes "cali boys" was a reference to Darin DOWD and Jacob DOWD. On July 14, 2021, Chief BUSHEY advised WIEDENHOEFT via text message that ATF agents were going to visit him that week. WIEDENHOEFT responded, "They're gonna call ufe (United Forces Enterprises) right no me. Personally." Chief BUSHEY explained it would be agents from Milwaukee and take less than an hour or hour and a half. WIEDENHOEFT and Chief BUSHEY exchanged the following text messages in summary:

- WIEDENHOEFT: Ok Should be routine I'm guessing
- WIEDENHOEFT: Should I make ufe available for a call

  [Affiant knows from this investigation that UFE is United Forces Enterprises]
- Chief BUSHEY: Perhaps
- WIEDENHOEFT: I'm gonna get a hold of them now
- WIEDENHOEFT: What time they coming Friday
- Chief BUSHEY: Around noonish

- Chief BUSHEY: Ok
- WIEDENHOEFT: They are in Hawaii and probably would not look good legally if they were on the call he says this is routine as its a weird round. Plus the f 16 joke may have aroused them lmfao.

  [Affiant knows from PayPal account information that packages have been addressed to Jacob DOWD in Kihei, Hawaii.]
- WIEDENHOEFT: Here is why the ammo
- WIEDENHOEFT: United Forces has surplus it doesn't not need anymore overseas. Instead of it sitting in a warehouse they have offered to donate this surplus ammunition the Law enforcement community. This ammunition can be used for precision shooting training, traded for equipment or used at auction to raise money for the department.
- Chief BUSHEY: Ok sounds good

22. Chief BUSHEY stated that he consulted the attorney, James B. Duquette, who represents the TLPD regarding the deal. Chief BUSHEY stated that Duquette approved of the deal. But in a September 16, 2021 interview with the Affiant, Duquette stated that he offered no opinion on the criminal legality of the proposed ammunition deal. He instead only offered an opinion regarding whether the police department could, as a matter of the law governing municipal contracts, enter an agreement to accept an ammunition donation. Duquette stated that he was under the impression the ammunition in question was to be used by the police department for training. He stated he never reviewed any of the documents in question. Chief BUSHEY did not tell

Attorney Duquette that the agreement was that TLPD would receive a cash payment in exchange for Chief BUSHEY signing and submitting a purchase order falsely indicating that armor piercing incendiary ammunition was to be imported for TLPD law enforcement use.

23. Chief BUSHEY also stated that he consulted the Town of Linn Town Board, which approved of the deal. Affiant has reviewed audio recordings of the Town of Linn Board meeting and a Protective Services Committee meeting that preceded it. During both meetings, Chief BUSHEY purported to describe the deal in question. He ultimately received approval from the Town Board to do the deal he described. The Town Board approved what was described to them as an agreement between the TLPD and a California FFL for the FFL to donate ammunition to the TLPD. Chief BUSHEY did not tell the Town Board or its Protective Services Committee that the agreement was that TLPD would receive a cash payment in exchange for Chief BUSHEY signing and submitting a purchase order falsely indicating that armor piercing incendiary ammunition was to be imported for TLPD law enforcement use.

24. Chief BUSHEY also stated that he sought approval from ATF before submitting the purchase order. Chief BUSHEY did call Industry Operations Inspector (IOI) Miguel Ruiz. During that call, Chief BUSHEY described a donation agreement very much like the agreement he described to the Town of Linn Board and Attorney Duquette. IOI Ruiz stated that Chief BUSHEY asked him if he could accept a donation of ammunition from UFE. IOI Ruiz advised Chief BUSHEY he was not certain if it was legal to accept a donation, but believed it was poor optics for a police chief to engage in that behavior.

25. Affiant interviewed Jason WIEDENHOEFT on September 3, 2021, after WIEDENHOEFT called and asked to speak about ammunition sales. WIEDENHOEFT stated that he had worked for Eli LAZAR selling ammunition for LAZAR's company, Alpha/Omega Brokerage. WIEDENHOEFT stated that Alpha Omega Brokerage, in turn, was hired by two brothers in California, Jacob and Darin DOWD to sell ammunition on behalf of their FFL (United Forces Enterprises).

26. WIEDENHOEFT stated that he was on a conference call with the DOWDs and LAZAR in which the DOWDs explained that they needed law enforcement contacts in order to be able to import certain "specialty ammo" that they could not otherwise legally import. WIEDENHOEFT stated that LAZAR was not then involved in any law enforcement deals and that WIEDENHOEFT stated he could arrange a deal through his friend, TLPD Chief BUSHEY. He also stated that he does not like LAZAR and does not believe he is a good person.

27. WIEDENHOEFT stated that he believed that once a police department ordered ammunition, including specialty ammunition, it could barter it. But Affiant asked WIEDENHOEFT if the DOWDs needed a law enforcement agency to indicate that the purchase order was for them because of the ammunition's armor piercing incendiary designation, and WIEDENOEFT replied "correct."

28. WIEDENHOEFT stated that "when I was first approached to sell, I was like this just doesn't sound right. You know, because I'm skeptical and, if it sounds too good to be true, but it was, everything is legit."

29. After the initial, in-person interview was completed, WIEDENHOEFT called the Affiant and stated that the DOWDs told him during the initial conference call

that it was necessary to acquire an exemption letter in order to import incendiary rounds. WIEDENHOEFT stated that he believed only law enforcement could import incendiary rounds, though he believed anyone could buy them.

30. WIEDENHOEFT stated that he prepared the template that BUSHEY used for the purchase order, and that BUSHEY emailed him the signed agreement. He stated he believes he FedExed the agreement to the DOWDs.

31. WIEDENHOEFT stated that he was paid by the DOWDs through LAZAR's company, Alpha Omega Brokerage.

32. WIEDENHOEFT made no mention of James COMPSTON during his interview, even when asked directly if anyone else was involved with him in law enforcement ammunition deals. Shortly after the interview with ATF, WIEDENHOEFT contacted the phone number 916-546-6309 on fourteen (14) occasions via text message. This phone number contains a area code for the Vacaville, CA, area.

33. Your affiant submitted a toll record/subscriber information subpoena to Verizon Wireless for the above number on 11/3/21. Your affiant received the records for the number 916-546-6309 on 11/8/21. The subscriber for the phone number is listed as Darin DOWD with an address of 7660 Hillhaven CT, Antelope, CA. Additionally, Verizon provided the email address for DOWD as darin.dowd@iCloud.com.

34. On September 15, 2021, Affiant interviewed James COMPSTON. Agents had contacted COMPSTON, and he invited agents to his home for the interview.

35. COMPSTON advised he was previously an Ohio State Trooper and was a member of the Columbus, Ohio, Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF) in 1998.

36. COMPSTON told agents he spoke with "Jason" (agents know this to be Jason WIEDENHOEFT, DOB: 07/1977) before the agents arrived. He advised WIEDENHOEFT was his partner in these ammunition deals. COMPSTON knew WIEDEHOEFT was interviewed by ATF approximately two (2) weeks ago. COMPSTON stated that WIEDENHOEFT told him: "Make sure you tell the ATF that I forgot to mention your name [during ATF's interview of WIEDENHOEFT], it wasn't intentional."

37. COMPSTON explained the agreed upon payment structure to agents. He advised that he was to split all sales 50/50 with WIEDENHOEFT no matter who closed the deal. This split was drawn from a 10 cents per round sale price. COMPSTON would have received a share from the Town of Linn Police Department deal with Chief BUSHEY.

38. COMPSTON stated that WIEDENHOEFT emailed him a purchase order to use with other departments and that COMPSTON proposed the purchase-order-for-donation exchange agreement to other police departments but had no takers.

39. COMPSTON stated that he had previously emailed with LAZAR but that he had deleted the email account he used to do so. He stated that he did not email with the DOWDs or WIEDENHOEFT.

40. COMPSTON also stated that he never directly corresponded with the DOWDs, and that they instead initially only corresponded with LAZAR but later corresponded directly with WIEDENHOEFT.

41. COMPSTON said that, in his view, U.F.E. (which he sometimes referred to as "HFE") would not bother to bring in 9mm, .40, .45. .308, 7.62x39 ammunition (i.e.,

non-specialty ammunition) by using law enforcement exemption letters because they can bring it in without law enforcement.

MILITARY SERVICE

42. During the interview of Chief BUSHEY, agents ascertained that WIEDENHOEFT used military affiliations in a manner to lend credibility to the business. Further, associating specialized units such as the United States Marine Corps (USMC) Scout Sniper suggested affiliation with an esteemed and advanced military unit. Subsequently, ATF contacted the United States Naval Criminal Investigative Service (NCIS) to validate these claims. Agents received the following information regarding the aforementioned members who did serve in the military:

- Joshua BESKE: Active member of the United States Army National Guard from January 1999 to January 2000. Active member of the USMC from December 2000 to June 2002. BESKE was discharged under other than honorable conditions and was separated for misconduct when a member who commits drug abuse, which is illegal, wrongful or improper use, possession, sale, transfer or introduction on a military installation of any narcotic substance, intoxicating inhaled substance, marijuana, or controlled substance, as established by 21 USC 812, when supported by evidence not attributed to urinalysis, supported by evidence not attributed to urinalyses administered for identification of drug abusers or to a member's volunteering for treatment under the drug identification and treatment program. This is an involuntary discharge directed in lieu of further proceedings or a convening board.
- Jason WIEDENHOEFT: was active-duty Army from October 1996 to July 1998.

He received an Honorable Discharge and was separated due to a personality disorder (Service initiated discharge directed by established directive when a personality disorder exists, not amounting to a disability which significantly impairs the member's ability to function effectively in the military environment). He is listed as a Disabled Veteran.

THE USE OF PAYPAL LINKED TO GMAIL ACCOUNTS

43. Affiant reviewed PayPal transactions and found that one of the PayPal Accounts of Darin DOWD was linked to email darindowdjr@gmail.com. Transactions were observed between DOWD and one of the PayPal accounts linked to United Forces Enterprises utilizing unitedforcesenterprises@gmail.com. Starting around January 1, 2020 until August 6, 2021 the DOWD account engaged in 29 sent transactions with the United Forces Enterprises account totaling approximately $178,351. Payment received from the account associated with United Forces Enterprises to the account associated with Darin DOWD over the same time-period totaled $357,726.23. Further, Affiant observed the PayPal account linked to darindowdjr@gmail.com engaged in approximately 29 payment sent transactions with the PayPal account associated Eli LAZAR utilizing a.elilazar@gmail.com totaling $97,722.68. Some of these transactions from Darin DOWD to LAZAR described the transaction as "executive dinner," "business yacht trip," "consulting fee," and "executive yacht and dinner trip UFE." Affiant knows from this investigation that "UFE" is an acronym for United Forces Enterprises. It is believed all of the above accounts and associated emails are vital to the operation of this business and the movement of funds.

44. Your Affiant reviewed the PayPal transaction log for the account

associated with Joshua BESKE utilizing slingshot187@gmail.com. On May 9, 2021, BESKE's account reflected a purchase for an item titled, "US CIA Special Agent Badge Solid Copper Replica Movie Props (4 optional) - CIA#767". Continuing on May 21, 2021, the PayPal linked to LAZAR and a.elilazar@gmail.com transferred #1,318.00 for "travel expenses". Affiant believes this replica special agent badge was bought before or around the time of a business trip conducted on behalf of Alpha Omega Brokerage/United Forces Enterprises.

USE OF ICLOUD and GMAIL BY THE GROUP

45. Affiant reviewed pen register trap and trace (PRTT) records associated with UNITEDFORCESENTERPRISES@GMAIL.COM from August 27, 2021 to October 26, 2021. The following is a summarization of the contacts:

- Darin.dowd@icloud.com: 4 contacts between 09/15/2021 and 09/29/2021 - this is believed to be the iCloud email address of Darin Dowd.
- Jakedowd@icloud.com: 3 contacts between 09/16/2021 and 10/26/2021- this is believed to be an email address for Jacob DOWD (W/M, DOB: 07/28/1993).
- darin@unitedforces.com: 85 contacts between 08/31/2021 and 10/26/2021 -this is a likely email address for Darin DOWD (W/M, dob: 05/19/1991).
- Enews@gunbroker.com: 40 contacts between 08/29/2021 and 10/24/2021 – this is a website for firearm purchases.
- Jaroslav.ciernava@btg.sk: 28 contacts between 09/06/2021 and 10/25/2021 - this is believed to be an employee email for a Slovakian ammunition company

- anthony@ammo-LLCcom: 17 contacts between 08/27/2021 and 09/30/2021 – this is believed to be an employee email from Ammo-LLC ammunition company.
- terrenceb@operation-defense.com: 14 contacts between 09/01/2021 and 09/16/2021 – this is believed to be an employee email address from an employee at Operation-Defense ammunition sales company.
- milesandsmiles@milesandsmiles.turkishairlines.com: 4 contacts between 09/04/2021 and 10/04/2021.
- members@members.gunbroker.com: 3 contacts between 08/27/2021 and 10/14/2021 – This is the membership email address for Gunbroker.com.

46. Your Affiant reviewed the PayPal registration information for United Forces Enterprises listed the user as Jacob Allen DOWD and a registered email of UNITEDFORCESENTERPRISES@GMAIL.COM. Further, United Forces Enterprises utilized UNITEDFORCESENTERPRISES@GMAIL.COM as their contact information on ATF Form 6 form ammunition importation.

BACKGROUND CONCERNING ICLOUD ACCOUNTS

47. You affiant obtained a Verizon Wireless toll record/subscriber subpoena for Darin DOWD's phone number. The subpoena listed the email account associated with DOWD as darin.dowd@icloud.com, as listed in paragraph 35.

48. Agents additionally served a subpoena to Robinhood for accounts associated with the DOWDs. The subpoena returns included an account in Darin DOWD's name with the listed account number as 106659477. The response also listed Darin DOWD's SSN (ending in 5149) (which is an accurate SSN for Darin DOWD) and

the email address as darin.dowd@icloud.com.

49. Lastly, agents received a subpoena response from ACORNS, an investment software application for Darin DOWD. Listed under account number 01551413061316 was the name Darin Dowd, address of 7660 Hillhaven Ct, Antelope, CA, and email address darin.dowd@icloud.com.

50. Based upon the three subpoena responses listed above, your affiant is confident the iCloud account listed in Attachment A is that of Darin DOWD.

INFORMATION CONCERNING FINANCIAL INSTITUTIONS

51. Your affiant is aware the target iCloud account (darin.dowd@iCloud.com) is linked to Darin DOWD's Citibank account #42028584300 and #42028584318. Your affiant observed some suspicious transactions located within Citibank's subpoena return which was received by investigators on 09/22/21. For example, on 11/19/20 United Forces Enterprises wrote a check for $100,000.00 to Darin DOWD which was deposited in the above account ending in 4318. Additionally, agents located several PayPal accounts utilizing the above listed iCloud account. Those accounts were observed depositing money in the Citibank account listed for Darin DOWD. On 11/19/20, agents observed a electronic debit receipt from Darin DOWD's CitiBank account into his Robinhood account for $50,000. Both accounts share the same email of darin.dowd@iCloud.com.

52. Agents additionally observed an Acorns Investment account for Darin DOWD linked to the email account darin.dowd@iCloud.com. DOWD lists his personal net worth on the registration page being $250,000 + along with his annual income listed as $250,000+. This account was approved on 11/18/2020. Agents obtained these results

from a grand jury subpoena that was provided by Acorns to agents on 09/23/21. On 04/03/2019, Darin DOWD filed Chapter 13 bankruptcy in the Eastern District of California listed under case number 19-22077. In that filing, Darin DOWD lists his net worth approximately between 0$ and $50,000. Darin DOWD listed his liabilities as $100,001-$500,000. Darin DOWD list his assets totaling $36,816.02 and his liabilities totalling $187,316.00. Lastly, Darin DOWD list his monthly income as $6,038.69. Your affiant considers the vast difference in income and net worth between the two years could be explained in the email account darin.dowd@iCloud.com.

53. On November 19, 2021, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) obtained a federal search warrant for the contents of the Apple iCloud account darin.dowd@iCloud.com. On December 1, 2021, the results were received by Case Agents and downloaded from Apple's online portal. The results located in the iCloud account contained videos, photos, emails, contact lists, and other electronic information. Case Agents began reviewing the information on or about 12/13/2021. Case Agents observed several posts concerning both Darin DOWD and Jacob DOWD (W/M, DOB: 07/28/1993) impersonating ATF federal agents.

54. Agents observed a video of the DOWD brothers getting into a physical altercation with unknown individuals on or about 2/12/2018. The altercation is believed to have occurred at Syntrol Heating, Air, Plumbing, Electricity, Solar at 2120 March Rd a, Roseville, CA. During the video, one of the DOWD brothers can be heard stating "I'm a federal fucking agent your done". The next video one individual is heard stating "we can arrest them it's all good", "I'm an ATF Special Agent" and "Put your hands behind your back". A screenshot of Jacob DOWD from the video is below:

55. The below photo depicts Darin DOWD with a fictitious ATF badge around his neck and was believed to be taken on 04/06/2018:

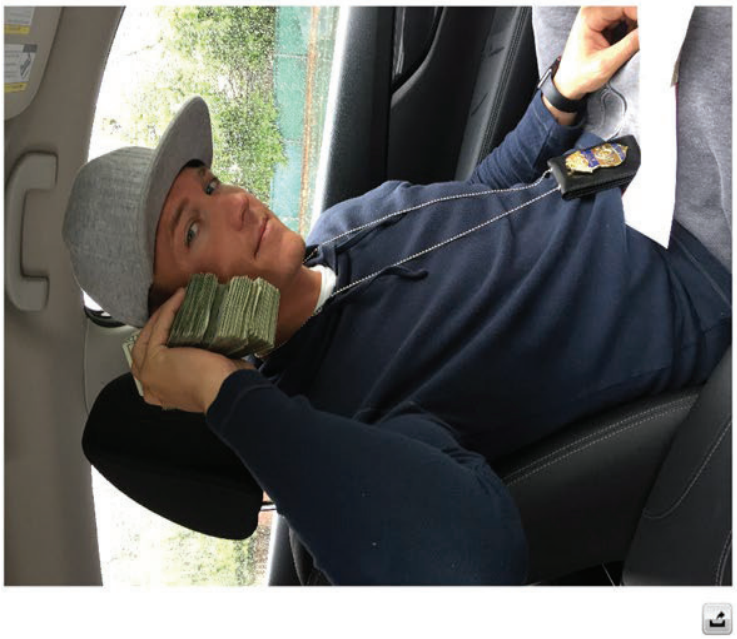

Image Information

File Name
IMG_1660.JPG

File Format
JPEG / JPG

File Size
2.12 MB

EXIF Provider Date
04/06/2018

EXIF Provider Time
11:47:07

EXIF Latitude
38.5321528

EXIF Longitude
-121.495553

Record Count
1

Hash Set Information

Hash Set Category

SHA-2
BF97FD79E99D8D4DFF2C14D6019FBE909958F4FF23898B84022062527CF5D688

MD5
FA3F6705D3964432019258202CDE7FED

Tags

Victim Identified

Offender Identified

Is Suspected

Is Distributed

Categorized by

Hash Set

56. Case Agents observed a video in which Darin DOWD can be heard talking to Jacob DOWD. The video depicts Jacob DOWD firing a Berretta handgun while wearing a "ATF Special Response Team" T-Shirt. Agents confirmed neither Jacob nor Darin DOWD have ever been employed with the ATF. Additionally, agents spoke with a member of the actual ATF Special Response Team who confirmed the shirt in the video had not been issued to team members in recent history. The video was captured on 07/29/2018 and a screenshot is depicted below:

57. Case Agents additionally analyzed emails within the iCloud account darin.dowd@icloud.com for correspondence associated with the trip to Peru in February of 2020. SA Connors located an email chain discussing the logistics, and insurance prices on $500,000 worth of firearms traveling from Peru to Rock Island, IL. The correspondence occurs between the above email account for Darin DOWD and two individuals associated with Edward J. Zarach & Associates, Inc. A customs brokerage and freight forwarding company based out of Elk Grove Village, IL. The emails occurred on 01/28/2020 and 01/29/2020.

58. Case Agents additionally located an email from darin.dowd@icloud.com to imaacs@state.gov on 02/28/2020. The email stated "Good morning, I am in need of a business visa for Peru. I have attempted to call as well as attempted to make an appointment in person. This is of urgent matter as I can not conduct business without it in Lima, Peru with the government. Please schedule me to come in to receive my business visa as soon as possible. Thank you, Darin Dowd".

59. This Court has previously authorized a warrant for information related to violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal Import of Ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); and 18 U.S.C § 545 (Smuggling).

60. Upon review of the returns from the abovementioned warrant, your affiant observed in plain view evidence of additional crimes, including the impersonation of an officer or employee of the United States (18 U.S. Code § 912) by Jacob DOWD and Darin DOWD and other known and unknown individuals. This application is for a warrant t seize and search evidence of the illegal impersonation of an officer or employee of the United States (18 U.S. Code § 912) by Darin DOWD and other known and unknown individuals in the iCloud return information already in the possession of the United States.. Based upon my training and experience and the evidence set forth above, I believe probable cause exists to search the electronically stored information described in Attachment A for evidence of those violations.

BACKGROUND CONCERNING APPLE

61. In my training and experience I have learned, Apple is a United States

company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

62. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari

web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

63. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users

can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

64. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

65. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on

Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

66. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

67. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets,

presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

68. Your affiant is aware that Darin DOWD's iCloud account is likely to contain electronic information such as messages, purchase orders, and customer lists for whom United Forces Enterprises was acquiring the Armor Piercing ammunition. The account darin.dowd@icloud.com and the evidence therein would accordingly be extremely useful to the investigation. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

69. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and

documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

70. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

71. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

72. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App

Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

73. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

74. There is probable cause to believe that in the Apple iCloud account for Darin DOWD listed as darin.dowd@iCloud.com to search the electronically stored information described in Attachment A for evidence of violations of the Foreign Corrupt Practices Act (15 U.S.C. 78dd-2(a)) and impersonating an officer or employee of the United States (18 U.S. Code § 912) by Darin DOWD and other known and unknown individuals.

REQUEST FOR SEALING

75. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an

opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with darin.dowd@iCloud.com that is currently within law enforcement custody at the ATF Milwaukee Field Office.

ATTACHMENT B
Particular Things to be Seized

1. Information to be disclosed by Apple (Provider)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved (reference number 6262734) pursuant to a request made under 18 U.S.C. § 2703(f) on July 21, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from 01/01/2021 to the present:

- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique

Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

- The contents of all emails associated with the account from 01/01/21 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- The contents of all instant messages associated with the account 01/01/21 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the

sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

- All records pertaining to the types of service used;
- All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal import of ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); and 18 U.S.C § 545 (Smuggling), those violations involving Darin DOWD and occurring after 01/01/21, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records containing the sale/purchase order of ammunition in a illegal format that is intended for the military/law enforcement that would not be for public use. Records can be contained in emails, text messages, SMS messages, iMessages, etc.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to the conspiracy and illegal importation of ammunition, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Signature